Canadian Journal of Law and Technology

Volume 12 | Number 1 Article 3

1-1-2014

# Atteinte à la vie privée et publicité comportementale

Virginie Blanchette-Séguin

# Atteinte à la vie privée et publicité comportementale

*Virginie Blanchette-Séguin*[*]

## INTRODUCTION

Ces dernières années, l'industrie des services en ligne a vu naître certaines sociétés phares, telles que Google, Twitter et Facebook, ayant en commun un modèle d'affaires selon lequel les services prodigués sont financés partiellement ou exclusivement par la publicité affichée sur le site de telle sorte qu'ils sont gratuits pour l'internaute qui les utilise.[1]

Or, en cette ère branchée de la communication, le modèle « classique » d'affichage de la publicité en ligne où tous les internautes sont exposés aux mêmes annonces perd de plus en plus de terrain au profit d'un nouveau type de publicité dite « ciblée ». Selon ce deuxième modèle, la publicité affichée dépendra du profil de l'internaute afin de s'inscrire dans ses champs d'intérêt propres. Cette seconde façon de faire présente un grand intérêt commercial puisqu'elle permet d'augmenter significativement l'effectivité de la publicité, soit le nombre de clics ou d'achats qui en découlent. En conséquence, la publicité ciblée est susceptible d'être facturée substantiellement plus cher aux annonceurs[2] et donc de générer plus de profit.

Le ciblage des internautes peut s'effectuer de diverses façons. Premièrement, certains sites déterminent la publicité qui sera affichée en fonction des caractéristiques personnelles que l'internaute aura lui-même divulguées, par exemple en se créant un profil sur le site en question ou en s'inscrivant à un service. Deuxièmement, il est possible d'afficher la publicité ciblée selon une analyse contextuelle. Les annonces seront alors en lien avec le contenu textuel de la page consultée ou,

---

[*] L'auteure est titulaire d'un LLB de l'Université de Montréal et d'un JD de la Osgoode Hall Law School. Le présent article a été rédigé dans le cadre du cours Protection des renseignements personnels et technologies de l'information du programme de LLM en droit des technologies de l'information de l'Université de Montréal. L'auteure tient à remercier Éloïse Gratton pour son soutien précieux. Toute erreur ou omission demeure toutefois entièrement attribuable à l'auteure.

1 Commission nationale de l'informatique et des libertés (CNIL), « La publicité ciblée en ligne », (Communication présentée en séance plénière le 5 février 2009, Paris, à la p 4), en ligne : CNIL <http://www.cnil.fr/ fileadmin/ documents/ La_CNIL/ actualite/Publicite_Ciblee _rapport_VD.pdf>; Commissariat à la protection de la vie privée au canada (CPVPC), *Rapport sur les consultations de 2010 du Commissariat à la protection de la vie privée du Canada sur le suivi, le profilage et le ciblage en ligne et sur l'infonuagique*, (mai 2011) à la p 15, en ligne : CPVPC <http://www.priv.gc.ca/resource/consultations/report_ 201105_f.pdf> [*Rapport sur les consultations de 2010*].

2 CNIL, *supra* note 1 à la p 4.

dans le cas d'un moteur de recherche, avec le mot clé saisi par l'internaute pour effectuer sa recherche. Troisièmement, selon une méthode autrement plus sophistiquée, les afficheurs peuvent sélectionner la publicité selon un profil très détaillé de la vie en ligne d'un individu en fonction de son historique de navigation sur une certaine période de temps. Ce type particulier de publicité ciblée se nomme « publicité comportementale ».[3]

Effectuer l'analyse inhérente à la présentation d'une publicité comportementale nécessite une quantité significative de renseignements sur l'internaute, tels que la nature des pages visitées, la fréquence de ces visites, le temps qui y est consacré, les interactions qui ont eu lieu, les achats qui ont été effectués ou les mots clés qui ont été saisis. Il s'agit de l'une des principales raisons qui ont poussé différents acteurs de l'Internet, qui se qualifient entre autres comme réseaux de publicité, à diversifier leurs services et leurs activités afin de suivre toujours plus étroitement les internautes et, ultimement, dresser le portrait le plus exhaustif possible de leur comportement.[4]

Le présent texte aura pour objet les questions relatives à la vie privée que soulève la publicité comportementale et le suivi des activités des individus qu'elle implique par définition. Pour ce faire, nous délimiterons d'abord le spectre du droit à la vie privée en droit québécois dans ce contexte (I.) et nous poursuivrons selon une approche plus critique en nous prononçant sur les différents arguments pouvant être soulevés quant à l'absence d'une perception humaine dans une violation potentielle du droit à la vie privée (II.)

## I. ÉTAT DES LIEUX : DROITS ET DOMMAGES EN MATIÈRE DE PUBLICITÉ COMPORTEMENTALE

Afin de délimiter le spectre québécois du droit à la vie privée, nous nous intéresserons tout d'abord à la portée de ce droit qui découle de l'application des lois pertinentes (I.(a)). Nous analyserons par la suite les différents types de dommages pouvant découler d'une atteinte au droit à la vie privée reliée à la publicité comportementale (I.(b)).

### (a) Textes législatifs applicables

Le droit à la vie privée, tel qu'il nous intéresse dans le cadre du présent travail, trouve sa source en droit civil québécois principalement dans trois instruments : la *Charte des droits et libertés de la personne*[5] (I.(a)(i)), le *Code civil du Québec*[6] (I.(a)(ii)) et la *Loi sur la protection des renseignements personnels dans le secteur privé*[7] (*LPRPSP*) (I.(a)(iii)) Sans y consacrer une sous-section, nous ferons également référence à la *Loi sur la protection des renseignements personnels et les doc-*

3 CNIL, *supra* note 1 à la p 5.

4 *Ibid.*

5 LRQ, c C-12 [Charte québécoise].

6 LQ, 1991, c 64 [*Code civil*].

7 LRQ, c P-39.1 [*LPRPSP*].

*uments électroniques*[8] en ce qu'elle est substantiellement similaire à la LPRPSP,[9] son équivalente québécoise.

### *(i) Charte des droits et libertés de la personne*

Consacré à l'article 5 de la Charte québécoise, le droit à la vie privée constitue l'un des droits de la personnalité les plus fondamentaux.[10] Fondé sur l'autonomie morale et physique des individus, le droit à la vie privée revêt une importance particulière puisqu'il est essentiel à leur bien-être.[11]

Défini de façon générale à la fin du 19e siècle par le juge américain Cooley comme étant « the right to be let alone »,[12] le spectre du droit à la vie privée est difficile à déterminer de façon précise. En effet, il a un caractère profondément subjectif et les activités protégées varient d'une personne à l'autre en fonction des circonstances et du rôle que l'individu concerné joue dans la société.[13]

Si le droit à la vie privée échappe encore à une définition formelle et systématique, il est toutefois possible d'identifier certaines de ses composantes : soit le droit à l'anonymat, à l'intimité, au secret et à la confidentialité.[14]

### *(ii)* Code civil du Québec

Le chapitre III du livre premier du *Code civil*, intitulé *Du respect de la réputation et de la vie privée* permet de préciser plus en avant la portée du droit à la vie privée. L'article 35 établit d'abord que toute personne a droit au respect de sa vie privée et qu'il ne peut y être porté atteinte sans son consentement à moins que la loi ne l'autorise.

L'article 36 ajoute en précision en énumérant certains actes qui peuvent être considérés comme des atteintes à la vie privée. Dans le contexte de notre étude de la publicité comportementale, nous nous intéresserons plus particulièrement aux exemples donnés aux paragraphes 2º, 4º et 6º :

> 2º Intercepter ou utiliser volontairement une communication privée;
>
> 4º Surveiller sa vie privée par quelque moyen que ce soit;
>
> 6º Utiliser sa correspondance, ses manuscrits ou ses autres documents personnels.

---

8 LC 2000, c 5 [loi fédérale].

9 Éloïse Gratton, « Chronique — Qu'est-ce qu'un renseignement personnel? Le défi de qualifier les nouveaux types de renseignements » (janvier 2013) *Repères*, *Droit civil en ligne* (DCL), EYB2013REP1287, aux p 3-4.

10 *Valiquette c. Gazette (The)*, [1997] R.J.Q. 30 (C.A. Que.), au para. 28; *Éditions Vice-Versa Inc. c. Aubry*, [1996] R.J.Q. 2137 (C.A. Que.); affirmed 1998 CarswellQue 4806, 1998 CarswellQue 4807 (S.C.C.).

11 *R. v. Dyment*, [1988] 2 R.C.S. 417 (S.C.C.) au para 17.

12 Samuel D Warren & Louis D Brandeis, « The Right to Privacy » (1890) 4-5 *Harv L Rev* 193, à la p 195.

13 Richard Jr La Charité, « Les droits de la personnalité », dans Barreau du Québec, *Personnes, famille et successions* — collection de droit 2012-2013, Cowansville, Yvon Blais, 2012, vol 3, à la section 2.E.1.

14 *The Gazette c. Valiquette*, *supra* note 10 au para 28.

À la lecture de ces exemples, il est manifeste que le législateur provincial n'avait pas l'intention à l'adoption de cet article en 1991 de régir la publicité comportementale, une industrie qui n'existait pour ainsi dire pas à cette époque. Il est malgré tout possible d'y déceler certains indices pertinents pour nos fins.

Tout d'abord, le paragraphe 4º de l'article 36 fournit une première indication quant à l'impact sur la vie privée d'une surveillance effectuée strictement par ordinateur. Les termes « par quelque moyen que ce soit » permettent effectivement de croire que l'interposition d'une machine entre l'entité qui effectue la surveillance et la personne surveillée ne pourrait pas constituer un élément permettant d'exclure une violation du droit à la vie privée.

Les paragraphes 2º et 6º de l'article 36 qui concernent la correspondance pourraient trouver application en matière de publicité ciblée dans les circonstances où les intérêts des internautes sont déduits de leurs communications privées tels que les courriels. Il s'agit d'une pratique déjà utilisée par Google qui, en effet, analyse le contenu des messages reçus par les détenteurs d'un compte Gmail pour déterminer la nature des annonces affichées en marge.[15]

Enfin, l'article 37 du *Code civil* prévoit que « toute personne qui constitue un dossier sur une personne doit avoir un intérêt sérieux et légitime à le faire. » Étant donné que la personnalisation de la publicité en ligne s'effectue grâce à la compilation de données relatives à l'historique de navigation de l'internaute, la constitution d'un dossier sur des personnes est une prémisse essentielle de la publicité comportementale. Cela étant, la question à se poser est la suivante : les réseaux de publicité en ligne ont-ils un intérêt légitime à constituer leurs dossiers sur les internautes? Nous traiterons de ce sujet dans la section portant sur la LPRPSP qui prévoit également l'obligation d'avoir un intérêt sérieux et légitime pour constituer un dossier sur une personne.

### *(iii)* Loi sur la protection des renseignements personnels dans le secteur privé *(LPRPSP)*

La loi sur la protection des renseignements personnels et les documents electroniques (LPRPDE) a pour objet de compléter le chapitre du *Code civil* portant sur la vie privée.[16] Tel que son nom l'indique, cette loi s'applique à la gestion des renseignements dits « personnels ». Nous nous demanderons donc, dans un premier temps, si les informations recueillies à l'occasion du traçage des internautes se qualifient comme renseignements personnels au sens de la LPRPSP (A). Dans un deuxième temps, nous analyserons la notion d'intérêt sérieux et légitime à constituer un dossier et le caractère nécessaire des informations collectées (B).

#### (A) Qualification de l'historique de navigation en tant que renseignement personnel

Selon l'article 2 de cette loi, un renseignement personnel s'entend de « tout renseignement qui concerne une personne physique et permet de l'identifier. » Dé-

---

15 CNIL, *supra* note 1 à la p 14; Richard A Posner, « Privacy, Surveillance and Law », (2008) 75-1 *U Chi L Rev* 245 à la p 249.

16 LPRPSP, *supra* note 7 à la art 1 al.1.

terminer si un renseignement se qualifie comme tel peut s'avérer être une tâche complexe pour laquelle il convient d'adopter une approche générale et contextuelle.[17]

Ainsi, pour savoir si la LPRPSP s'applique dans le contexte particulier de la publicité comportementale, il faut tout d'abord déterminer si les renseignements recueillis à l'occasion du traçage (ou le marqueur permettant de suivre l'internaute) constituent des données permettant d'identifier un individu. Dans l'affirmative, les réseaux de publicité en ligne seront alors soumis aux exigences établies par la LPRPDE.[18]

Une des problématiques liées à cette qualification est que les réseaux de publicité ne suivent pas directement les individus, mais plutôt des adresses IP ou des marqueurs déposés sur les ordinateurs. Or, ces derniers peuvent être utilisés par plusieurs individus[19] comme c'est le cas avec les ordinateurs familiaux ou, à plus forte raison encore, les ordinateurs mis à la disposition du public dans les bibliothèques ou les cafés Internet. Toutefois, selon l'approche générale qu'il convient d'utiliser, il ne faut pas laisser ces cas particuliers qui relèvent de l'exception miner le reste de l'analyse.

Effectivement, le traçage effectué par les réseaux publicitaires cible le plus souvent un individu qui, s'il n'est pas formellement identifié, est malgré tout identifiable.[20] Par exemple, en 2006, AOL avait publié à des fins scientifiques une liste qui recensait les 20 millions de mots clés qu'avaient saisis 650 000 utilisateurs anonymes dans son moteur de recherche pendant une période de trois mois. Or, il s'est révélé possible d'identifier certains des individus qui correspondaient aux profils anonymes en examinant l'ensemble des recherches effectuées.[21]

En ce qui a trait aux renseignements issus du traçage des internautes, à l'occasion de l'analyse relative à savoir s'il s'agit de renseignements personnels selon la définition prévue l'article 2 (1) de la loi fédérale (qui est substantiellement

---

17 CPVPC, *Rapport sur les consultations de 2010*, *supra* note 1 à la p 27.

18 CPVPC, Fiche d'information, « Lorsque le moindre de vos gestes est surveillé . . . Les annonceurs font un suivi de vos comportements (2011), en ligne » : CPVPC <http://www.priv.gc.ca/resource/fs-fi/02_05_d_52_ba_01_f.asp> [Lorsque le moindre de vos gestes est surveillé].

19 Éloïse Gratton, « Personalisation, Analytics, and Sponsored Services: The Challenges of Applying PIPEDA to Online Tracking and Profiling Activities », (2010) 8-2 *CJLT* 297 à la p 298 [Personalisation, Analytics and Sponsored Services].

20 Eric Cormier, *L'industrie de l'omniscience : le profilage comportemental et le droit à la vie privée au Canada*, mémoire de maîtrise, Ottawa, Faculté de droit, Université d'Ottawa, 2012 à la p 14, en ligne : Université d'Ottawa <http://www.ruor.uottawa.ca/en/bitstream/handle/10393/20680/Cormier_Eric_2012_these.pdf?sequence=1>; Janet Lo, *« A "Do Not Track List" for Canada? »* (2009) à la p 52, en ligne : Public Interest Advocacy Centre <http://www.piac.ca/privacy/tracking_consumers_online_behavioural_targeted_advertising_and_a_do_not_track_list_in_canada/>.

21 Nate Anderson, « AOL realises search data on 500,000 users (updated) » (7 août 2006), en ligne : ArtTechnica <http://arstechnica.com/uncategorized/2006/08/7433/>; E Cormier, *supra* note 20 à la p 61; É Gratton, « Personalisation, Analytics, and Sponsored Services », *supra* note 19 à la p 299.

similaire à la définition donnée par la législation provinciale[22]), le Commissariat à la protection de la vie privée du Canada[23] affirme que :

> Bien qu'on avance souvent que les renseignements recueillis sur les activités en ligne sont anonymes et qu'ils ne permettent pas d'identifier une personne, des rapports publiés récemment ont révélé que les données parfois présumées comme étant anonymes peuvent être associées à nouveau à une personne en particulier, et ce, avec une certaine facilité. De plus, la combinaison de données provenant de profils en ligne anonymes à des données provenant d'autres sources, comme les sites de réseautage, augmente les risques que des profils anonymes en ligne soient associés à des identités hors ligne.[24]

Par ailleurs, à l'occasion de son récent rapport d'enquête sur les pratiques du géant de l'Internet Google,[25] le Commissariat a appliqué différents principes de la loi fédérale dans un contexte d'une plainte liée à l'affichage de publicité comportementale en ligne. Ainsi, malgré le fait que le rapport ne contienne malheureusement pas une analyse détaillée et systématique de la notion de renseignements personnels,[26] il a néanmoins le mérite de dissiper les doutes qui pouvaient subsister quant à la qualification de l'historique des activités en ligne comme renseignements personnels.

En définitive, le Commissariat, le Groupe de travail de l'Article 29 et plusieurs auteurs arrivent à la conclusion que les renseignements recueillis à l'occasion du traçage des activités en ligne des individus constituent des renseignements personnels.[27] Nous poursuivrons donc notre analyse du cadre légal concernant la publicité comportementale en y appliquant la LPRPSP.

---

22 É Gratton, « Personalisation, Analytics, and Sponsored Services », *supra* note 19 à la p 298.

23 Ci-après « Commissariat » ou « CPVPC ».

24 CPVPC, Fiche d'information, *Publicité comportementale*, (2011), en ligne : <http://www.priv.gc.ca/ resource/fs-fi/02_05_ d_52_ba_02_f.asp>.

25 CPVPC, *Rapport de conclusions — L'utilisation par Google de renseignements sensibles sur l'état de santé aux fins de l'affichage de publicités ciblées soulève des préoccupations en matière de vie privée*, (2014) nº2014-001, en ligne : CPVPC <http://www.priv.gc.ca/cf-dc/2014/2014_001_0114_f.asp>.

26 *Ibid*, au para 28.

27 CPVPC, *La protection de la vie privée et la publicité comportementale en ligne*, Lignes directrices, (2012) à la p 2, en ligne : CPVPC <http://www.priv.gc.ca/information/guide/2011/gl_ba_ 1112_f.pdf>; Groupe de travail « article 29 » sur la protection des données, « Avis 2/2010 sur la publicité comportementale en ligne », Adopté le 22 juin 2010, nº 00909/10/FR, WP 171 à la p 3, en ligne : Europa <http://ec.europa.eu/ justice/policies/privacy/docs/wpdocs/2010/wp171_fr.pdf>; E Cormier, *supra* note 20, à la p 52-56; É Gratton, « Qu'est-ce qu'un renseignement personnel? », *supra* note 9 à la p 12; J. Lo, *supra* note 20 à la p 52.

### (B) Intérêt sérieux et légitime de constituer un dossier sur des personnes

L'article 4 de la LPRPSP prévoit, tout comme l'article 37 du *Code civil*, qu'un intérêt sérieux et légitime est nécessaire afin de constituer un dossier sur une personne. La nature de ce qu'est un intérêt sérieux et légitime à constituer un dossier n'est cependant pas précisée par la loi.[28]

Afin de faire échec au raisonnement assumant que les entités commerciales ont l'intérêt requis pour constituer un dossier sur leurs clients, il a déjà été soutenu par des organisations de défense des intérêts des consommateurs que, dans le contexte de la publicité comportementale, les internautes étaient davantage un produit que des clients puisque les revenus des réseaux de publicité dépendent de la collecte du plus grand nombre possible de renseignements personnels. Selon cette logique, les annonceurs seraient les réels clients. Les tenants de cette thèse affirmaient que cette situation compromettait l'intérêt sérieux et légitime des réseaux de publicité à se constituer un dossier sur les internautes.[29]

Nous ne considérons pas que cette analyse puisse tenir. En effet, la publicité en ligne occupe une place excessivement importante dans le fonctionnement de l'industrie d'Internet. Elle permet d'ailleurs à de très nombreux sites d'offrir des services gratuitement aux internautes.[30] D'ailleurs, en 2009, dans l'analyse d'une plainte formulée à l'encontre de Facebook, Elizabeth Denham, commissaire adjointe à la protection de la vie privée du Canada, a considéré que la possibilité de présenter de la publicité aux utilisateurs était une considération essentielle, et non pas secondaire, à la viabilité de ce modèle d'affaire.[31] Ainsi, nous croyons que les réseaux de publicité en ligne ont l'intérêt sérieux et légitime nécessaire au sens des articles 4 de la LPRPSP et 37 du *Code civil* afin de se constituer un dossier sur les internautes.

### (C) Information collectée doit se limiter à ce qui est nécessaire

Finalement, selon l'article 9 (1º) de la LPRPSP et le principe 4.3.3. de la loi fédérale, les entités collectant des renseignements personnels doivent se limiter à l'information qui leur est nécessaire. La jurisprudence a d'ailleurs interprété les termes « fins nécessaires » comme signifiant les fins indispensables.[32]

Dans le contexte de la publicité comportementale, il est difficile de déterminer quels renseignements sont réellement nécessaires à la réalisation de cette activité. Plus de renseignements seront recueillis, plus les profils seront détaillés et plus la publicité pourra coïncider avec les intérêts réels de l'internaute.

---

28 R Jr La Charité, *supra* note 13 à la note 119.

29 CPVPC, *Rapport sur les consultations de 2010*, *supra* note 1 à la p 16.

30 CNIL, *supra* note 1.

31 CPVPC, *Report of Findings Into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) Against Facebook Inc. Under the Personal Information Protection and Electronic Documents Act*, nº 2009-008, (2009) au para 131, en ligne : CPVPC <http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.asp> [*Report of Findings Into the Complaint Against Facebook*].

32 *X. c. Le Groupe Jean-Coutu (PJC) inc.*, JE 2000AC-63 (CQ).

Dans la plainte contre Facebook déjà mentionnée, la collecte des renseignements étant nécessaire pour fournir le service gratuitement aux internautes, le Commissariat a jugé que l'information recueillie était essentielle à l'entreprise sans reprocher à la société d'en collecter trop.[33] L'information qui est « nécessaire » aux fins des réseaux de publicité en ligne afin de personnaliser la publicité présentée aux internautes peut donc être comprise très largement.

En définitive, la LPRPSP, à l'instar de la loi fédérale, permet d'établir un certain équilibre entre la protection de la vie privée des individus et les avantages, notamment économiques, à ce que les entreprises aient accès à des renseignements personnels. À ce propos, dans l'arrêt *Englander c. TELUS Communications Inc.*, la Cour d'appel fédérale affirme que :

> L'objet de la LPRPDE est (. . .) certes axé sur la protection de la vie privée des personnes, mais il se rapporte aussi à la collecte, à l'utilisation et à la communication de renseignements personnels par les organisations. Cet objet est de faire en sorte que lesdites collecte, utilisation et communication soient exécutées d'une manière qui concilie, dans toute la mesure du possible, le droit de la personne à la vie privée et les besoins de l'organisation. Il y a donc deux intérêts concurrents dans l'objet de la LPRPDE : le droit de la personne à la vie privée d'une part, et le besoin commercial d'accès aux renseignements personnels d'autre part.[34]

## (b) Types de dommage résultant d'une atteinte à la vie privée

L'existence d'un dommage ne se présume pas du seul fait d'une atteinte au droit à la vie privée, bien que celui-ci soit un droit fondamental prévu par la Charte québécoise. Aussi, il est nécessaire d'en faire la preuve selon la règle normale de prépondérance des probabilités.[35] Deux types de dommages peuvent découler d'une atteinte à la vie privée causée par la publicité comportementale : les dommages objectifs (I.(b)(i)) et les dommages subjectifs (I.(b)(ii))

### *(i) Dommages objectifs*

Les dommages objectifs découlant d'une atteinte à la vie privée font référence à une utilisation inattendue et non désirée de renseignements personnels contre l'individu auquel ils se rapportent.[36] Or, le traçage des internautes peut constituer un outil pour effectuer une prise de décision les concernant.[37]

En effet, afin de maximiser le profit généré par chaque transaction, une entité collectant de l'information sur l'historique de navigation des individus peut utiliser les renseignements recueillis pour moduler les prix de certains produits ou services

---

33 *Report of Findings Into the Complaint Against Facebook*, *supra* note 31 au para 131.

34 *Englander v. TELUS Communications Inc.*, 2004 CAF 387 (F.C.A.) au para 38.

35 *The Gazette c. Valiquette*, préc., note 10 au para 25; *Éditions Vice-Versa Inc. c. Aubry, CA*, *supra* note 10.

36 Ryan Calo, « The Boundaries of Privacy Harm », (2011) 86 *Ind L J* 1131 à la p 1131.

37 J Lo, *supra* note 20 à la p 53.

en fonction de l'intérêt ou de la capacité d'achat présumés des personnes suivies.[38] Ainsi, les internautes identifiés comme étant prêts à payer un prix supérieur à la normale subiraient un préjudice économique quantifiable se qualifiant comme un dommage objectif résultant d'une atteinte à la vie privée. Malheureusement, cette situation ne relève pas de la science-fiction et constitue une réelle possibilité. Il y a quelques années, la société de commerce électronique Amazon a été soupçonnée de moduler les prix de la marchandise vendue sur sa plate-forme en fonction du profil des utilisateurs.[39]

Cette pratique présente un grand intérêt économique pour les sociétés pratiquant le commerce en ligne puisqu'elle augmente encore leur rapport de force face aux consommateurs.[40] Elle est toutefois très mal perçue par ces derniers qui la jugent, avec raison selon nous, discriminatoire et socialement inappropriée[41] malgré le fait que certaines personnes puissent être avantagées par cette méthode de fixation des prix. Paradoxalement, les meilleurs clients d'une entreprise, soit ceux qui effectuent le plus d'achats en ligne et ceux qui lui sont les plus fidèles, seraient probablement les premiers à subir un préjudice.[42]

En outre, le profilage pourrait également permettre d'exclure certains types de consommateurs. Par exemple, les clients issus des classes les moins aisées de la société, qui statistiquement sont plus susceptibles de porter plainte et de ne pas être fidèles au commerçant, pourraient devenir la cible de mesures dissuasives[43] ou figurer sur des listes répertoriant les consommateurs jugés indésirables.[44] Le profilage en ligne pourrait donc devenir un vecteur de la discrimination envers les groupes

---

38 Éloïse Gratton, *Understanding Personal Information: Managing Privacy Risks*, Markham, LexisNexis Canada, 2013, à la p 382.

39 CNIL, *supra* note 1 à la p 14; É Gratton, *Understanding Personal Information*, *supra* note 38 à la p 382; Anita Ramasastry, « Web Sites Change Prices Based on Customers' Habits » (24 juin 2005), en ligne : CNN <http://www.cnn.com/2005/LAW/06/24/ramasastry.website.prices/>.

40 Janet D Gertz, « The Purloined Personality: Consumer Profiling in Financial Services » (2002) 39 *San Diego L Rev* 943 aux p 964-965.

41 A Ramasastry, *supra* note 39.

42 É Gratton, *Understanding Personal Information*, *supra* note 38 à la p 382; George Hariton, John Lawford & Hasini Palihapitiya, *Radio Frequency Identification and Privacy: Shopping into Surveillance*, Ottawa, Public Interest Advocacy Centre, 2006, à la p 20, en ligne : PIAC <http://www.piac.ca/privacy/radio_frequency_identification_rfid_and_privacy_shopping_into_surveillance+print>.

43 É Gratton, *Understanding Personal Information*, *supra* note 38 aux p 383-384; Chris J Hoofnagle & Kerry E Smith, *Debunking the Commercial Profilers' Claims: A Skeptical Analysis of the Benefits of Personal Information Flows*, Washington, Electronic Privacy Information Center, FTC, nº P034102, 2003, aux p 20-21.

44 Anthony Danna & Oscar H Gandy, Jr, « All That Glitters is Not Gold: Digging Beneath the Surface of Data Mining », (2002) 40 *Journal of Business Ethics* 373 à la p 381.

qui sont déjà socialement désavantagés[45] et mettre inéquitablement en évidence certains traits « négatifs » des individus.[46]

En plus du risque que les prix des biens et services en ligne soient adaptés en fonction d'un profil virtuel, on peut imaginer des situations où un service serait tout simplement refusé sur la base des informations reliées au profil d'un internaute. Par exemple, un prêt pourrait être refusé par le service en ligne d'une institution financière en raison de la situation économique présumée d'un internaute. Sinon, une personne homosexuelle ou atteinte de certaines maladies pourrait devenir susceptible de se voir refuser l'octroi d'une assurance-vie.[47]

Ainsi, les renseignements personnels d'un internaute, déduits à partir d'un suivi de ses activités en ligne, pourraient être utilisés pour prendre une décision défavorable à son égard. Cette situation constitue en soi un problème puisque l'entité effectuant le traçage a eu accès à une information, peut-être non pertinente, que le principal intéressé ne souhaitait pas lui communiquer. De surcroît, les renseignements utilisés aux fins de la prise de décision sont potentiellement inexacts.[48] Le problème est par ailleurs exacerbé par le fait que ce processus est effectué à l'insu de l'individu concerné[49] qui ne peut donc s'y opposer ou faire rectifier les informations erronées.

### *(ii) Dommages subjectifs*

Les dommages subjectifs découlant d'une atteinte à la vie privée font référence à l'impression importune d'être sous une surveillance non-désirée.[50] Ils comprennent le sentiment de perte de contrôle, de l'embarras ou de l'humiliation qui peuvent découler de cette surveillance pour l'individu observé. L'auteur Richard A. Posner compare cette sensation avec celle d'être vu nu par des étrangers dans les sociétés occidentales. Même s'il n'en résulte pas de conséquences concrètes, l'individu exposé pourrait potentiellement être très embarrassé.[51]

Selon la thèse soutenue par Ryan Calo, le dommage subjectif découlant de l'impression d'être observé peut survenir même en l'absence d'une observation réelle,[52] par exemple si une caméra aveugle est pointée vers un individu.[53] En cela, l'analogie avec la prison panoptique imaginée par les frères Bentham est intéressante. Dans cet établissement carcéral, une tour centrale permettrait aux gardiens de surveiller les prisonniers sans toutefois être vus par eux. L'idée est que, ne sachant

---

45 Oscar H Gandy, Jr, « Exploring Identity and Identification in Cyberspace », (2000) 14 *Notre Dame J L Ethics & Pol'y* 1085 aux p 1107-1108.

46 Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford, Stanford University Press, 2010, à la p 79.

47 É Gratton, « Personalisation, Analytics, and Sponsored Services », *supra* note 19 à la p 298.

48 CPVPC, *Rapport sur les consultations de 2010*, *supra* note 1 à la p 16.

49 *Ibid.*

50 R Calo, *supra* note 36 à la p 1131.

51 R Posner, *supra* note 15 à la p 245.

52 R Calo, *supra* note 36 à la p 1146.

53 *Ibid*, à la p 1147.

pas s'ils sont surveillés à un moment précis, les détenus finiront par agir en tout temps comme si le regard des gardiens était braqué sur eux.

La surveillance (ou l'impression de surveillance[54]) a une incidence importante sur le comportement humain. D'abord, elle augmente significativement l'autocensure et l'inhibition.[55] Ensuite, une surveillance persistante peut créer de l'anxiété et de l'inconfort chez l'individu en question.[56] De fait, elle constitue un important outil de contrôle, les normes sociales étant beaucoup plus rigoureusement respectées quand les personnes sont observées. Ainsi, si un niveau raisonnable de surveillance est bénéfique pour l'ordre social, un niveau trop élevé aura un impact négatif sur la liberté de choix et l'autodétermination.[57]

Dans le cas particulier de la publicité comportementale, un dommage subjectif pourrait, hypothétiquement, découler du simple fait qu'un internaute voit s'afficher des annonces relatives à l'objet de recherches antérieures de nature privée. Il pourrait alors ressentir une impression importune d'être surveillé puisqu'il réalise que lesdites recherches ont été analysées et sont conservées pour utilisation future. Ce traitement ayant été effectué strictement par des systèmes informatiques, donc en l'absence de toute implication d'une personne humaine capable de jugement, nous considérons que le dommage subjectif découlant du sentiment d'observation serait dans ce cas infime, voire inexistant tel qu'il sera discuté dans la sous-section II.(a).

Le principal dommage subjectif susceptible d'être occasionné par la publicité comportementale est la divulgation de renseignements personnels. Il existe un risque que l'information déduite de l'historique de navigation soit dévoilée à un tiers parce que celui-ci se trouvait à proximité de l'internaute en question au moment de l'affichage de la publicité ou parce que l'annonce apparaît sur un instrument partagé par plusieurs personnes,[58] tel qu'un ordinateur familial.

L'existence du dommage subjectif et son étendue, donc du sentiment désagréable découlant de la surveillance, dépendront de la nature plus ou moins sensible de l'information dévoilée. En effet, la divulgation de certains renseignements, déjà connus ou de nature non sensible, ne risque pas de créer un préjudice quelconque. Par exemple, une divulgation effectuée par le biais d'une publicité relative à des vêtements ou à d'autres articles de consommation courante ne porte pas *a priori* préjudice à la personne concernée.

Cependant, la divulgation de renseignements personnels de nature sensible peut créer un dommage subjectif important. Ainsi, le dévoilement de l'état de santé d'une personne affectée d'une maladie particulièrement stigmatisante peut être excessivement dommageable. De la même façon, les croyances religieuses, les affiliations politiques, les affaires amoureuses ou sexuelles et les considérations financières peuvent revêtir un caractère strictement privé et sont par conséquent

---

54 Daniel J Solove, « A Taxonomy of Privacy », (2006) 154-3 *U Pa L Rev* 477 à la p 495.

55 E Cormier, *supra* note 20 à la p 23; D Solove, « A Taxonomy of Privacy », *supra* note 54 à la p 493.

56 D Solove, « A Taxonomy of Privacy », *supra* note 54 à la p 493.

57 Paul M Schwartz, « Privacy and Democracy in Cyberspace », (1999) 52 *Vand L Rev* 1609, à la p 1656; D Solove, « A Taxonomy of Privacy », *supra* note 54 à la p 494.

58 É Gratton, *Understanding Personal Information*, *supra* note 38 à la p 382.

susceptibles d'engendrer un dommage subjectif pour l'internaute si elles sont divulguées à des tiers suite à l'affichage de publicité comportementale.

## II. IMPACTS DE LA PUBLICITÉ COMPORTEMENTALE SUR LA VIE PRIVÉE

Après avoir ainsi délimité le spectre du droit à la vie privée en droit québécois dans le contexte de la publicité comportementale, nous considérerons l'impact sur la vie privée de la surveillance des internautes inhérente à cette pratique dans la perspective où celle-ci est effectuée strictement par des ordinateurs. Dans cette section, nous nous pencherons sur les arguments des tenants de la thèse selon laquelle cette analyse ne porte pas atteinte à la vie privée (II.(a)) puis sur les arguments inverses (II.(b))

### (a) Arguments selon lesquels la surveillance liée à la publicité comportementale ne porte pas atteinte à la vie privée

Les arguments que nous avons recensés au soutien de la thèse selon laquelle la surveillance liée à la publicité comportementale ne porte pas atteinte à la vie privée des internautes sont les suivants : une atteinte à la vie privée implique nécessairement l'implication d'une personne humaine (i), la surveillance liée à la publicité comportementale était connue et acceptée (ii) et, finalement, recevoir de la publicité, même non désirée, ne constitue pas une atteinte à la vie privée (iii).

#### *(i) Une atteinte à la vie privée implique nécessairement l'implication d'une personne humaine*

Selon plusieurs auteurs, une atteinte à la vie privée présuppose nécessairement l'implication d'une personne humaine. De façon implicite, Richard B. Parker adhère à cette proposition en définissant la vie privée comme étant le « control over who can sense us. »[59]

Afin de prouver que le seul traitement de renseignements personnels par des ordinateurs ne constitue pas en soi une atteinte à la vie privée, Eric Goldman propose l'exemple suivant : un système informatique génère une liste identifiant tous les hommes séropositifs vivant au Texas, d'origine latino-américaine et âgés de plus de 40 ans. Cette liste serait couplée avec leur adresse, leur numéro de sécurité sociale et leur date de naissance. Il va sans dire que cette information est hautement sensible. Toutefois, plutôt que de s'afficher sur un écran ou d'être imprimé, le document est immédiatement détruit. Les individus concernés ne subiraient, dans ce cas, aucun préjudice. Selon le professeur Goldman, cette situation hypothétique est la preuve que le seul traitement de l'information par un ordinateur ne constitue pas une atteinte à la vie privée s'il ne s'accompagne d'aucune utilisation contre l'individu auquel les renseignements se rapportent.[60]

---

59 Richard B Parker, « A Definition of Privacy », (1973) 27 *Rutgers L Rev* 275 à la p 280.

60 Eric Goldman, « Data Mining and Attention Consumption », dans Katherine J Standburg & Daniela S Raicu, *Privacy and Technologies of Identity*, New York, Springer Science and Business Media, 2006, 225 à la p 228.

Orin S. Kerr et Richard A. Posner avancent un raisonnement similaire relativement à la « recherche » de renseignements personnels. Ils affirment respectivement que :

> The best answer is that a search occurs when information from or about the data is exposed to possible human observation, such as when it appears on a screen, rather than when it is copied by the hard drive or processed by the computer.[61]

> Computer searches do not invade privacy because search programs are not sentient beings. Only the human search should raise constitutional or other legal issues.[62]

Ainsi, en l'absence de connaissance par un être sensible capable de jugement, la surveillance serait beaucoup moins invasive et ne pourrait donc pas porter atteinte à la vie privée des internautes. Selon Daniel J. Solove, c'est la possibilité d'être jugé par une autre personne qui engendre l'atteinte à la vie privée :

> Being observed by an insect on the wall is not intrusive for privacy; rather, privacy is threatened by being subject to *human* observation, which involves judgments that can affect one's life and reputation.[63]

Dans le contexte de la publicité comportementale, nous sommes en accord avec ces auteurs en ce qui concerne le traitement initial de l'information par les ordinateurs des sociétés de publicité. Seul, il ne porte pas atteinte à la vie privée des internautes.

La distinction qu'il y a à faire avec l'impression de surveillance que peut avoir un individu fixé par une caméra aveugle est que, dans ce cas, celui-ci pense qu'il est potentiellement observé par un être humain. Dans le cas de la publicité comportementale, un internaute ne peut pas raisonnablement craindre qu'une personne quelque part analyse ses activités en ligne personnelles afin de lui présenter une publicité adaptée à ses intérêts.

Par ailleurs, il est hautement improbable que l'information relative aux internautes soit examinée par une personne au sein des sociétés de publicité après avoir été traitée initialement grâce à un algorithme par un ordinateur. D'une part, la quantité d'information recueillie est colossale. D'autre part, ces entreprises n'ont aucun intérêt à s'immiscer dans la vie privée des internautes ou à souiller leur réputation.[64]

Or, tel qu'il sera plus amplement discuté dans la sous-section II.(b), subséquemment à l'analyse impersonnelle des données, il est possible qu'une divulgation ou une utilisation soit faite des renseignements personnels, et ce, toujours sans qu'une personne humaine n'intervienne de quelque façon que ce soit. Aussi, nous considérons qu'il est faux d'affirmer qu'il ne peut jamais y avoir de violation du

---

61 Orin S Kerr, « Searches and Seizure in a Digital World », (2005) 119 *Harv L Rev* 531 à la p 551.

62 R Posner, *supra* note 15 aux p 253-254.

63 Daniel J Solove, « Privacy and Power: Computer Databases and Metaphors for Information Privacy », (2000) 53 *Stan L Rev* 1393 à la p 1418.

64 D Solove, « Privacy and Power », *supra* note 63 à la p 1418.

droit à la vie privée si l'information est simplement traitée par des systèmes informatiques.

*(ii) La surveillance était connue et acceptée*

À l'instar de Ryan Calo, nous sommes d'avis qu'il n'y a pas de dommage subjectif résultant d'une surveillance qui était connue et acceptée, voire désirée.[65] Il y aurait un argument à faire à l'effet que la publicité comportementale ne porte pas atteinte à la vie privée puisque la surveillance inhérente à la publicité comportementale est connue des internautes et acceptée par ceux-ci puisqu'elle leur est bénéfique.

Il est possible d'arguer que la surveillance est connue, car elle est divulguée dans les politiques d'utilisation des services utilisés par les internautes. Cependant, ces politiques n'étant généralement pas lues et comprises, il est inévitable que le traçage s'effectue souvent à l'insu des personnes concernées.[66] Par ailleurs, bien qu'un grand nombre d'internautes soient au courant qu'ils sont tracés dans leur navigation en raison de l'omniprésence de la publicité comportementale sur la toile, très peu d'entre eux ont conscience de l'étendue et des impacts possibles de ce suivi.[67]

En ce qui concerne l'acceptation de la surveillance, l'octroi du consentement des internautes se fait actuellement principalement selon un système de type *opt-out*. Ainsi, en l'absence d'un refus, l'acceptation des individus au suivi est présumée. Leur choix se limite, la plupart du temps, à accepter les conditions relatives à un service ou à s'abstenir de l'utiliser.[68] À ce propos, le Commissariat à la protection de la vie privée du Canada se dit « préoccupé par le risque d'atteinte à la vie privée que présentent ces pratiques [de traçage des activités en ligne], notamment en ce qui a trait à leur manque de transparence et à la qualité du consentement obtenu. »[69]

En outre, bien qu'il existe certains outils permettant aux internautes de réduire le suivi dont ils font l'objet (par exemple en bloquant l'installation de *cookies* sur leur ordinateur), ceux-ci ne procurent qu'une protection partielle[70] et il peut être compliqué et fastidieux de les mettre en place ou de les utiliser.[71]

Certains acteurs de l'Internet affirment que la publicité comportementale est bénéfique aux internautes puisqu'elle personnalise l'expérience de navigation en ligne selon leurs préférences et leur évite d'être exposés à une masse de contenu qui ne présente pour eux aucun intérêt.[72] De plus, les revenus découlant de la pub-

---

65 R Calo, *supra* note 36 à la p 1142.

66 É Gratton, « Personalisation, Analytics, and Sponsored Services », *supra* note 19 à la p 298; J Lo, *supra* note 20 à la p 49.

67 E Cormier, *supra* note 20 à la p 1.

68 CPVPC, *Lorsque le moindre de vos gestes est surveillé*, *supra* note 18.

69 CPVPC, *Publicité comportementale*, *supra* note 24.

70 CPVPC, *Lorsque le moindre de vos gestes est surveillé*, *supra* note 18.

71 J Lo, *supra* note 20 à la p 50.

72 CPVPC, *Lorsque le moindre de vos gestes est surveillé*, *supra* note 18; E Goldman, *supra* note 60 à la p 234; J Lo, *supra* note 20 à la p 48.

licité comportementale financent une multitude de services en ligne. Ainsi, elle permet indirectement aux internautes d'y avoir accès gratuitement.[73]

En effet, nombre de personnes affirment apprécier recevoir de l'information ciblée en fonction de leurs champs d'intérêt.[74] Or, il est loin d'être établi que la surveillance effectuée par les réseaux de publicité est acceptée par la communauté des internautes dans son ensemble. Deux études réalisées au Canada dans les dernières années permettent de conclure que les Canadiens ne sont pas l'aise avec l'idée que les réseaux de publicité suivent leur comportement en ligne.[75] Selon certaines organisations de protection des intérêts des consommateurs, la publicité comportementale serait au mieux tolérée par les internautes.[76]

Dans ces circonstances, nous pensons qu'il est difficile d'affirmer que les internautes ont consenti à ce que leurs activités en ligne soient suivies par les réseaux de publicité et qu'ils ne peuvent donc, de ce fait, subir de dommage subjectif lié à la publicité comportementale.

### *(iii) Recevoir de la publicité, même non désirée, ne constitue pas une atteinte à la vie privée*

Selon le *Lindop Report on Data Protection* paru en Angleterre en 1978, seule une minorité de la population considérait que la publicité non désirée constitue une intrusion dans leur vie privée. Il s'agirait donc d'une pratique tout à fait acceptable.[77] Toutefois, nous considérons que les conclusions tirées de ce rapport sont difficilement applicables à la publicité comportementale.

Premièrement, le contexte prévalant à l'époque était très différent de celui qui existe aujourd'hui. La publicité non désirée dont il était question alors ne résultait pas d'une surveillance exhaustive des activités privées des individus ce qui, dans notre cas, constitue une donne importante à considérer. Deuxièmement, la perception de ce que constitue la vie privée n'est pas fixe. Au contraire, cette notion varie dans le temps et est différente selon les sociétés considérées.[78] À ce propos, faut-il rappeler que l'Angleterre est l'un des États où il y a le plus de caméras de surveillance dans les endroits publics?[79]

---

73 CNIL, *supra* note 1 à la p 4; CPVPC, *Lorsque le moindre de vos gestes est surveillé*, *supra* note 18; CPVPC, *Rapport sur les consultations de 2010*, *supra* note 1 à la p 15; J Lo, *supra* note 20 à la p 48.

74 CPVPC, *Lorsque le moindre de vos gestes est surveillé*, *supra* note 18; CPVPC, *Rapport sur les consultations de 2010*, *supra* note 1 à la p 15.

75 *Infra*, p 19.

76 CPVPC, *Rapport sur les consultations de 2010*, *supra* note 1 à la p 16.

77 Norman Lindop, *Report of the Committee on Date Protection*, Cmnd.7341, HMSO, Londres, 1978, au para 1711; É Gratton, *Understanding Personal Information*, *supra* note 38 à la p 353.

78 *The Gazette c. Valiquette*, *supra* note 10 au para 30.

79 Christian Laval, « Surveiller et prévenir. La nouvelle société panoptique », (2012) 2-40 *Rev du MAUSS* 47 à la p 60.

### (b) Arguments selon lesquels la surveillance liée à la publicité comportementale peut potentiellement porter atteinte à la vie privée

Les arguments que nous avons recensés au soutien de la thèse selon laquelle la surveillance liée à la publicité comportementale peut potentiellement porter atteinte à la vie privée des internautes sont les suivants : une partie importante de la population ressent un malaise envers cette surveillance (i), il existe un risque de divulgation des renseignements personnels collectés (ii) et, finalement, il existe également un risque que ces renseignements soient utilisés contre les internautes (iii).

#### *(i) Malaise des internautes envers la publicité comportementale*

Une étude réalisée au Canada en 2009 par le Public Interest Advocacy Centre (PIAC) révèle que près du trois quart des répondants n'étaient pas à l'aise avec la publicité fondée sur le suivi des activités en ligne.[80] Un autre sondage, celui-ci effectué pour le compte de l'Association canadienne de marketing, conclut que la moitié des Canadiens sont plutôt mal à l'aise à l'idée que des spécialistes du marketing utilisent des renseignements sur la navigation des consommateurs pour leur présenter des publicités plus pertinentes.[81]

Ce malaise de la population face à la publicité comportementale s'est d'ailleurs traduit, en mars 2004 dans l'État américain d'Utah, en une loi interdisant aux sociétés de publicité de présenter certains types de publicité ciblée, et ce, même si l'individu concerné y consentait.[82] Cette loi fut toutefois invalidée en juin 2004 puisqu'elle venait à l'encontre de la liberté de commerce.[83]

En ce qui concerne le sentiment négatif des internautes face au suivi de leurs activités en ligne, même le professeur Daniel J. Solove, qui considère que c'est la possibilité d'être jugé par une autre personne qui engendre l'atteinte à la vie privée,[84] précise que la surveillance effectuée par le biais d'une collecte informatique de données n'est pas sans conséquence :

> I do not, however, want to discount the dangerous effects of surveillance through the use of databases. Although the purposes of the users of personal data are generally not malignant, databases can still result in unintended harmful social effects.[85]

Certains auteurs considèrent encore que la publicité comportementale constitue une violation de la vie privée en ce qu'elle peut inculquer à un individu des

---

80 J Lo, *supra* note 20 à la p 11.

81 CPVPC, *Lorsque le moindre de vos gestes est surveillé*, *supra* note 18; CPVPC, *Rapport sur les consultations de 2010*, *supra* note 1 à la p 16.

82 *Utah Spyware Control Act*, HB 323, 2004 General Session, Part 2 (Utah 2004); E Goldman, *supra* note 60 à la p 234.

83 *WhenU.com Inc. v. Utah*, Civil Doc. No 0407097578 (Utah Dist Ct., June 22, 2004); E Goldman, *supra* note 60 à la p 234.

84 Daniel J Solove, *The Digital Person: Technology and Privacy in the Information Age*, New York, New York University Press, 2004 à la p 35.

85 *Ibid.* à la p 15.

croyances, des intentions ou des désirs[86] et qu'ainsi, elle serait de nature à la manipuler et à restreindre son autonomie.[87]

Cependant, avec Eric Goldman,[88] nous considérons que le seul fait que les systèmes informatiques des réseaux de publicité en ligne traitent les renseignements personnels des internautes ne constitue pas en soi une atteinte à leur vie privée. En l'absence de toute perception humaine capable de jugement, on ne peut parler d'une réelle surveillance susceptible de produire les effets d'inhibition sur le comportement précédemment décrits.[89]

Dans l'affaire *Blais c. La Société des Loteries Vidéos du Québec inc.*, il fut pris en considération que les messages électroniques de l'employé n'étaient pas lus par ses responsables. Le courriel problématique dans cette affaire avait été porté à l'attention de ses supérieurs seulement après avoir été bloqué par le *firewall* protégeant le système informatique de l'entreprise.[90] Cette décision suggère que le traitement passif des messages par un système électronique ne constituait pas une atteinte à la vie privée de l'employé. De même, nous soutenons que le traçage des activités en ligne ne constitue pas en soi une atteinte à la vie privée des internautes.

### *(ii) Risque de divulgation de renseignements personnels*

Tel qu'exposé dans la sous-section I.(b)(ii) portant sur les dommages subjectifs, la publicité comportementale expose les internautes au risque de voir leurs renseignements personnels dévoilés à des tiers. Quand l'information divulguée n'est pas de nature sensible, aucun dommage ne sera subi. Par contre, quand il s'agit de renseignements personnels de nature sensible, les personnes concernées peuvent subir un dommage subjectif, la divulgation pouvant les faire ressentir de la honte, de l'embarras ou de la gêne ou même entrainer d'autres conséquences dans leur vie personnelle.

Par exemple, en 2006, à l'occasion de la publication d'AOL mentionnée précédemment[91] de la liste des mots clés utilisés par des profils anonymes, il était possible d'avoir accès à des recherches portant sur des sujets extrêmement sensibles tels que le suicide ou l'inceste. D'autres pouvaient être associées à des intentions criminelles, comme la saisie des termes « comment tuer sa conjointe » jumelée avec des requêtes concernant des photos d'accidents de voiture ou de

---

86 Jason Millar, « Core Privacy: A Problem for Predictive Data Mining », dans Ian Kerr, Valerie Steeves & Carole Lucock, dir, *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*, New York, Oxford University Press, 2009, 103 à la p 119.

87 Tal Z Zarsky, « Desperately Seeking Solutions: Using Implementation-Based Solutions for the Troubles of Information Privacy in the Age of Data Mining and the Internet Society », (2004) 56-1 *Maine Law Review* 14, aux p 30-31, 38.

88 E Goldman, *supra* note 60 à la p 228.

89 *Ibid.* à la p 12.

90 *Blais c. Société des Loteries Vidéos du Québec Inc.*, 2003 QCCRT 0014 (Que. L.R.B.) aux paras. 28, 92.

91 Anderson, *supra* note 2 à la p 6.

cadavres.[92] Cela illustre bien que l'historique de navigation d'un individu peut comprendre des détails intimes sur sa vie privée et à quel point sa divulgation peut se révéler dommageable pour lui.

Quand les annonces portent sur des questions sensibles telles que l'orientation sexuelle ou les affiliations politiques, le Groupe de travail de l'Article 29[93] et certains groupes de protection des intérêts des consommateurs[94] considèrent que la pratique de la publicité comportementale devrait être découragée et procéder selon un système de type *opt-in*, donc avec le consentement préalable express des internautes visés.

Avec ces groupes, nous soutenons qu'exiger un réel consentement positif des individus avant de les exposer à de la publicité comportementale reliée à des sujets sensibles serait une mesure raisonnable. N'affectant pas le consentement nécessaire à la diffusion de la publicité liée aux renseignements non sensibles, cette mesure constituerait une entrave minimale à l'industrie de la publicité, mais diminuerait significativement les risques d'atteinte à la vie privée des individus. À ce propos, il est intéressant de noter que le principe 4.3.6 prévu à l'annexe 1 de loi fédérale prévoit que :

> La façon dont une organisation obtient le consentement peut varier selon les circonstances et la nature des renseignements recueillis. En général, l'organisation devrait chercher à obtenir un consentement explicite si les renseignements sont susceptibles d'être considérés comme sensibles. Lorsque les renseignements sont moins sensibles, un consentement implicite serait normalement jugé suffisant.

Dans son rapport du 14 janvier 2014, la commissaire à la protection de la vie privée du Canada reprochait essentiellement à Google de ne pas avoir respecté ces directives concernant la qualité du consentement nécessaire afin de procéder à l'affichage de publicité comportementale liée à des renseignements personnels, nommément l'état de santé de l'internaute. Considérant qu'il s'agit indubitablement d'une donnée sensible, un consentement explicite de la personne concernée aurait été nécessaire.[95]

S'il est très clair que certains renseignements sont de nature sensible, l'analyse peut se révéler plus ardue pour d'autres. D'ailleurs, certains renseignements ne seront sensibles que dans des circonstances particulières ou s'ils sont couplés avec une autre information.[96] Ainsi, la qualification des renseignements sera une première difficulté de mise en œuvre de ce système mixte de consentement *opt-in* pour les renseignements sensibles et *opt-out* pour les autres.

Une autre façon de limiter les risques de divulgation des renseignements sensibles serait de permettre qu'ils soient utilisés aux fins de publicité comporte-

---

92 E Cormier, *supra* note 20 à la p 61; Omer Tene, « What Google Knows: Privacy and Internet Search Engines », (2008) 4 *Utah L Rev* 1433 à la p 1718.

93 Groupe de travail « article 29 » sur la protection des données, *supra* note 27 à la p 23; É Gratton, *Understanding Personal Information*, *supra* note 38 à la p 356.

94 CPVPC, *Rapport sur les consultations de 2010*, *supra* note 1 à la p 28.

95 CPVPC, *Rapport de conclusions*, *supra* note 25 aux para 26-29.

96 E Cormier, *supra* note 20 à la p 50; É Gratton, *Understanding Personal Information*, *supra* note 38 à la p 353.

mentale seulement quand l'individu ciblé est connecté à un compte personnel relié à ces renseignements. Premièrement, puisque l'individu se serait préalablement identifié grâce à son mot de passe, les chances sont minimes que la publicité soit reçue par une autre personne partageant le même ordinateur.[97] Deuxièmement, les annonces relatives à ces renseignements personnels n'apparaîtront pas à des moments inopportuns. En effet, ce n'est pas parce qu'un individu s'est connecté, par exemple, à sa boîte de messagerie usuelle qu'il est disposé à recevoir des annonces sur des médicaments contre le sida ou à caractère sexuel dévoilant potentiellement des détails de sa vie intime. Peut-être se trouve-t-il dans un lieu public ou en compagnie d'autres personnes à qui il ne souhaite pas divulguer certaines informations.

Somme toute, si nous considérons que le traçage des internautes ne leur fait pas subir un dommage subjectif significatif, nous sommes cependant d'avis qu'il les expose à un risque de dévoilement de leurs renseignements personnels. Or, cette divulgation est susceptible de constituer une atteinte à leur vie privée et de leur faire subir un dommage subjectif. Aussi, il convient de prendre les mesures pertinentes afin de minimiser ce risque sans toutefois restreindre indûment les activités des sociétés de publicité en ligne qui jouent un rôle important dans l'industrie de l'Internet.

### *(iii) Risque de dommage objectif*

En plus d'exposer les internautes à un risque de dommage subjectif, le traçage des activités des individus en ligne crée pour eux un risque de dommage objectif, donc d'utilisation inattendue et non désirée de leurs renseignements personnels. En effet, nul besoin qu'un être humain n'intervienne pour qu'une décision défavorable soit « prise » à l'encontre d'un individu.[98] Par exemple, les systèmes informatiques du *Terrorist Security Administration* pouvaient lister des individus dans une « Do not fly list » sans qu'un être humain ne confirme la pertinence de cette décision.[99]

Tel qu'exposé dans la sous-section I.(b)(i), un dommage subjectif peut survenir dans le contexte de la publicité comportementale quand les entreprises modulent le prix des biens et services vendus en ligne en fonction des profils des internautes qu'elles auront établis grâce à leur historique de navigation. Certains types de consommateurs jugés indésirables pourraient également se voir exclus. Selon nous, cette situation constitue en soi un problème puisque l'entité effectuant le traçage a eu accès à des renseignements personnels, peut-être non pertinents, que le principal intéressé ne souhaitait pas lui communiquer.

De surcroît, selon le professeur Oscar H. Gandy, la discrimination des consommateurs effectuée grâce au profilage serait essentiellement fondée sur des présomptions erronées puisque la complexité de l'identité d'une personne humaine ne peut être réduite aux caractéristiques prédéterminées recensées par les systèmes informatiques.[100]

---

97 É Gratton, *Understanding Personal Information*, *supra* note 38 à la p 355.

98 Danielle K Citron, « Technological Due Process », (2007) 85 *Wash U L Rev* 1249 à la p 1253.

99 D Citron, *supra* note 98 à la p 1253, à la note 22.

100 E Cormier, *supra* note 20 à la p 25; D Solove, *The Digital Person*, *supra* note 85 à la p 181.

Même sans s'aventurer dans de telles considérations philosophiques, la discrimination des consommateurs sur la base des profils prédictifs générés par des ordinateurs fait peser sur les individus le risque d'une utilisation contre eux d'une information potentiellement inexacte.[101] En effet, les profils électroniques autoconstitués se sont révélés être souvent truffés d'inexactitudes.[102] Or, ce problème est exacerbé par le fait que la décision est prise à l'insu du principal intéressé.[103] Celui-ci n'a donc pas l'opportunité de rectifier l'information utilisée contre lui.[104]

En plus du risque de prise de décision défavorable à l'individu par l'entité effectuant le traçage ou par une entreprise légitime ayant acheté les renseignements, les internautes se voient également exposés à un risque de bris de sécurité des systèmes informatiques où sont stockés leurs renseignements personnels et donc au danger de vol d'identité et de fraude qui en découle.

Le risque de bris de sécurité des banques de données commerciales est bien réel. Pour ne donner qu'un exemple, en février 2005, le courtier de données ChoicePoint a vendu des dossiers comprenant les renseignements personnels d'environ 145 000 Américains à des criminels se faisant passer pour des entreprises légales. Au moins 750 vols d'identité se soldant par une fraude totale de plus d'un million de dollars furent attribués à ce seul bris de sécurité.[105]

Ainsi, le traçage des internautes inhérent à la publicité comportementale expose les internautes à un risque que leurs renseignements personnels ne soient utilisés contre eux soit dans le contexte d'une discrimination systématique des consommateurs présentant un certain profil ou alors, en raison d'un bris de sécurité potentiel. Dans la situation où l'un de ces risques se concrétisait, nous considérons que les individus concernés subiraient alors un dommage objectif et une atteinte à leur droit à la vie privée.

## III. CONCLUSION

La publicité comportementale, en raison des gains d'efficacité qu'elle permet de réaliser,[106] est devenue le standard de l'industrie de la publicité en ligne et est aujourd'hui omniprésente sur internet.[107] Dans la mesure où l'information collectée

---

101 CPVPC, *Rapport sur les consultations de 2010*, *supra* note 1 à la p 16; Philippa Lawson, *Techniques of Consumer Surveillance and Approaches to their Regulation in Canada and the USA*, Ottawa, Canadian Internet Policy and Public Interest Clinic (CIPPIC), 2005, à la p 7, en ligne : CIPPIC <http://www.idtrail.org/files/Techniques%20of%20Consumer%20Surveillance%20w% 20 footnotes.pdf>; J Lo, *supra* note 20 à la p 51.

102 P Lawson, *supra* note 101 à la p 7.

103 CPVPC, *Rapport sur les consultations de 2010*, *supra* note 1 à la p 16; J Lo, *supra* note 20 à la p 51.

104 P Lawson, *supra* note 101 à la p 7.

105 E Cormier, *supra* note 20 à la p 16; Matt Hines, « LexisNexis Break-in Spurs More Calls for Reform » (9 mars 2005), en ligne : CNET News <http:// news.cnet.com /LexisNexis-break-in-spurs-more-calls-for-reform/ 2100-1029_3-5606911.html>; P Lawson, *supra* note 101 à la p 7.

106 CNIL, *supra* note 1 à la p 4.

107 J Lo, *supra* note 20 à la p 4.

n'est ni divulguée ni utilisée pour prendre une décision défavorable à l'égard des individus auxquels elle se rapporte, nous considérons que la publicité comportementale ne constitue pas en soi une atteinte à la vie privée des internautes. Celle-ci leur est même bénéfique en ce qu'elle améliore leur expérience de navigation en ligne et finance certains des services qu'ils utilisent.

Cependant, la réalité est que la publicité comportementale crée un risque que des renseignements personnels, potentiellement de nature hautement sensible, soient divulgués ou utilisés à l'encontre des personnes concernées. En cela, la publicité comportementale crée un risque d'atteinte à la vie privée même si elle ne constitue pas en soi une atteinte à ce droit. Ainsi, nous arrivons à la conclusion qu'il est tout à fait possible qu'une atteinte à la vie privée ait lieu sans qu'une personne humaine n'intervienne de quelque façon que ce soit.

La publicité comportementale est régie par des lois qui ont été rédigées à une époque où elle ne constituait pas encore un enjeu. Or, face au risque d'atteinte à la vie privée qu'engendre cette pratique, il conviendrait de la règlementer de façon précise notamment afin d'éviter que l'information collectée lors du suivi des activités des internautes ne soit utilisée afin de prendre une décision défavorable à leur égard. En outre, la publicité comportementale ne devrait pouvoir porter sur des sujets sensibles que si la personne concernée y a expressément consenti. Ces modifications législatives auraient le double avantage d'assurer une meilleure protection de la vie privée des internautes et d'éviter une perte de confiance de la population face au commerce électronique.

La technologie ayant tendance à avoir une longueur d'avance sur le droit,[108] il est fondamental de réformer la législation encadrant la publicité comportementale, et l'Internet de façon générale, afin qu'elle soit en adéquation avec la réalité et que les innovations technologiques ne se fassent pas au prix d'un recul des droits fondamentaux.

---

108 P Lawson, *supra* note 101 à la p 8.